PRIVACY IMPACT ASSESSMENT

VISA APPLICATION MANAGEMENT SYSTEMS (VAMS)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Visa Application Management Systems. Includes Diversity Visa Information System (DVIS); electronic Document Processing (eDP) & eDP Web; Immigrant Visa Allocation Management System (IVAMS); Immigrant Visa Information System (IVIS); and Pre Immigrant Visa Overseas(IVO) Technology (PIVOT).

(b) Bureau: Consular Affairs (CA)

(c) System acronym: VAMS

(d) iMatrix Asset ID Number: VAMS 258572; DVIS 17; eDP 5091, eDP Web 5092; IVAMS 97; IVIS 49; PIVOT 6654

(e) Reason for performing PIA: Click here to enter text.

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization – consolidation of paperwork for legacy systems

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
VAMS is currently undergoing its initial Assessment and Authorization (A&A) [as a consolidated boundary system] in order to receive an Authorization to Operate (ATO) status. The estimated ATO date is March 2018. All systems in the consolidated boundary are included in this Privacy Impact Assessment (PIA).

(c) Describe the purpose of the system:

VAMS - is a logical business grouping of Visa Application Management Systems for Consular Affairs, which consists of Diversity Visa Information System (DVIS), Electronic Document Processing (eDP) and eDP Web, Immigrant Visa Allocation Management System (IVAMS), Immigrant Visa Information System (IVIS), and Pre IVO Technology (PIVOT).

DVIS: Supports the State Department's administration of the Diversity Immigrant Visa (DV) program, a program provided by law to promote immigration from countries with historically low rates of immigration to the United States. The program creates an internet-based "lottery" and randomly selects individuals from a pool of eligible entrants and qualifies them to apply for immigrant visas.

eDP: The electronic Data Processing (eDP) is a smart-client Windows application that is installed on National Visa Center (NVC) workstations. It allows users to scan, attach, view, edit, or delete immigrant visa (IV) documentation received at the NVC. The eDP mission requirements, in support of the Bureau of Consular Affairs (CA), are to do the following:

- To receive immigrant visa supporting documents electronically and store them to the Consular Consolidated Database (CCD) so that posts can view them.
- To provide an interface to scan the paper files received at the NVC and store them electronically.

Documentation uploaded at the NVC is replicated to the CCD at frequent intervals to allow posts to view supporting documentation.

eDP Web: The web component (eDP Web Central and eDP Web Post) is used by all the posts and external agencies such as the Department of Homeland Security (DHS) to view the immigrant visa (IV) documents related to IV cases. The post user is able to retrieve and view all documents associated to a case or an applicant in a printable report format. eDP Web Central is available as a menu item in a CCD report. eDP Web Post can be accessed from either IVO or post CCD portal.

IVAMS: Supports the Bureau of Consular Affairs mission requirements as an inventory system for immigrant visas (IV) and diversity visas (DV). IVAMS tracks the CA overseas posts' requests for and allocations of immigration and diversity visas. IVAMS deals with numbers of visas as opposed to individual visas and their associated applicant names.

IVAMS performs the following basic functions for both immigrant and diversity visas:

- Receives allocation requests from posts.
- Allocates visas and prepares the emails to send allocation numbers to posts.
- Performs analysis and generates reports on visa allocation activities.

- Processes monthly workload.

There is one basic difference in the way immigrant visas and diversity visas are processed:

- Demand for immigrant visas is processed by comparing a priority date assigned to each request with a cut-off date.
- Demand for diversity visas is processed by comparing a rank number assigned to each request with a cut-off rank number.
- Demand data from posts is entered into IVAMS manually or by receiving demand data through email from posts, which is then entered into the IVAMS database through the application.

IVIS: Used by the National Visa Center (NVC) to manage the processing of immigrant visa petitions received from the Department of Homeland Security (DHS) - United States Citizenship and Immigration Services (USCIS) regional service centers and district offices. IVIS provides for the recording of petitioner and beneficiary data, the processing of cases based on priority and cut-off dates, the creation and recording of correspondence with the beneficiary, petitioner and/or agent and the transmittal of data to the Immigrant Visa Overseas (IVO) system at post for final processing.

The mission of IVIS is to assist the NVC in tracking and processing immigration visa petitions based on local necessities and requirements established by the State Department. The immigrant visa issuance process begins with the submission of a petition for immigration to USCIS. USCIS reviews and adjudicates the petition and forwards approved petitions to the State Department for visa processing. Using IVIS, the NVC performs visa-processing activities that track petitions requesting immigration services from initial NVC receipt from USCIS through transfer to posts.

PIVOT: The Pre Immigrant Visa Overseas Technology (PIVOT) information system supports immigrant visa (IV) pre-processing at the National Visa Center (NVC), which includes immigrant visa case creation, immigrant visa package review, and support and inquiry functions. PIVOT interfaces with Consular Electronic Application Center (CEAC), electronic Document Processing (eDP), and Enterprise Appointment Management System (EAMS) to achieve paperless pre-processing for IV applications. When pre-processing is completed, PIVOT cases are transferred overseas for adjudication in the Immigrant Visa Overseas (IVO) system (iMatrix-817). This is a custom developed Hypertext Markup Language (HTML) and Procedural Language / Structured Query Language (PL/SQL) application available on the Department's intranet (OpenNet) through the CCD website. All interfaces are brokered through CCD and Consular Affairs Enterprise Service Bus (CAESB) services, including the following examples:

- Petition data received from USCIS;
- Case data and messages sent to and collected from CEAC;
- IV interview appointment scheduling information received from EAMS in response to PIVOT requests.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The following details the PII collected on U.S. citizens/Legal Permanent Residents (LPRs) and what is collected on non-U.S. citizens/non-LPRs. The PII is required to facilitate and adjudicate the processing of petitions for visa appplications.

DVIS - Collects the following information on U.S. citizens, LPRs and aliens:

- Names of individuals
- Birthdates of individuals
- Phone numbers of individuals
- Business addresses
- Personal addresses
- Email addresses
- Images or biometric identifiers (IDs)

eDP Client - Displays the following information on U.S. citizens, LPRs and non-citizens/non-LPRs:

- Name (Last, First, Middle) & Alias(es)
- Spouse & Child(ren) Name (Last, First, Middle) & Alias(es)

eDP Web - Displays the following information on U.S. citizens, LPRs and non-citizens/non-LPRs:

- Name (Last, First, Middle) & Alias(es)
- Spouse & Child(ren) Name (Last, First, Middle) & Alias(es)
- Birthdate (applicant, spouse, child(ren)) – in digitized image
- Birthplace (applicant, spouse, child(ren)) – in digitized image
- Social Security number (SSN) or other identifying number (Alien or A number) – in digitized image

IVAMS- Collects the following information on non-citizens/non-LPRs

- Names of individuals
- Birthdates of individuals

***Note**: The data IVAMS collects is not covered by the Privacy Act so the remainder of this document will not address this system.*

IVIS - Collects the following information on U.S. citizens, LPRs and non-citizens/non-LPRs

- Names of individuals
- Personal address
- E-mail address(es) of individuals
- Phone number(s) of individuals
- Birthdates of individuals
- Gender
- Marital Status
- Alien number
- SSN
- Tax Identification Number (TIN)
- Substantive medical information
- Substantive legal information
- Substantive family information
- Substantive educational information
- Organization name/Business address
- U.S. Status as citizen or alien
- Nationality
- City & country of birth
- Substantive individual financial information (Income Information for Joint Sponsors)
- Images or biometric IDs

PIVOT: Collects information on U.S. citizens, LPRs and non-citizens/non-LPRs

- Name
- Birthdate
- Birthplace
- SSN
- Phone number
- Personal address
- e-mail address
- Images and/or biometric IDs
- Financial information about applicants and case sponsors
- Legal information
- Names and birthdates of applicant's spouse & children
- Marriage place and date

- Names of applicant's parents
- Dates of applicant's previous travel to the United States
- Education information
- Employment information

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

COLLECTIVE LIST (to reduce redundancy):

- 8 U.S.C. §§ 1151-1363a (Title II of the Immigration and Nationality Act of 1952, as amended);
- 8 C.F.R. § 245.1(a)
- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. § 2651a (Organization of the Department of State);
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 26 U.S.C. § 6039E (Information Concerning Resident Status)
- Immigration Act of 1990, PL 101-649, November 29, 1990 (an Act to amend the Immigration and Nationality Act of 1952)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996, PL 104-208, Div. C, September 30, 1996
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, September 30, 1996
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107–56, October 26, 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002, PL 107-174, May 14, 2002
- Child Status Protection Act of 2002, PL 107–208, August 6, 2002 (an Act to amend the Immigration and Nationality Act of 1952)
- Anti-Drug Abuse Act of 1988, PL 100–690, November 18, 1988
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: Visa Records – STATE-39

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): October 25, 2012

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number Department of State Records Disposition Schedule:
  A-14-001 Visa Records, B-09-001 and 002 Consular Records

- Length of time the information is retained in the system:
  The length of time a record will be kept is dependent on the specific item and the applicable rules in A-14-00, B-09-001 and 002 of the State Department records rentention schedule. Records in these systems are retained on an average of 25 years or when it is determined that they are longer needed.

- Type of information retained in the system:
  Visa Records may include information regarding the following individuals when required by a visa application: U.S. petitioners and U.S. persons (Legal Permanent Residents) applying for returning resident travel documentation.

  CATEGORIES OF RECORDS IN THE SYSTEM: Visa Records maintains visa applications and related forms; biometric information; photographs; birth, marriage, death and divorce certificates; documents of identity; interview worksheets; biographic information sheets; affidavits of relationship; medical examinations and immunization reports; police records; educational and employment records; petitions for immigrant status and nonimmigrant status; bank statements; communications between the Visa Office, the National Visa Center, the Kentucky Consular Center, U.S. embassies, U.S. consulates general and U.S. consulates, other U.S. government agencies, international organizations, members of Congress, legal and other representatives of visa applicants, relatives of visa applicants, and other interested parties where such communications are, or may be, relevant to visa adjudication; and internal Department of State correspondence and notes relating to visa adjudication. Visa Records may also contain

information collected regarding applicant's or petitioner's U.S. family members; U.S. employers; other U.S. persons referenced by the applicant or petitioner.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?
Collective List to reduce redundancy
26 USC§ 6039E – Information Concerning Resident Status
8 USC§§1101-1503 Title II of the Immigration and Nationality Act of 1952, as amended

(b) How is the information collected?

DVIS: The original source of the information in the Diversity Visa Information System (DVIS) is the application that is entered into the Electronic Diversity Visa Application Entry System (eDV/AES). (Note: eDV is not within the boundary of VAMS). DVIS is not accessed directly by the public. For cases that are selected for further processing, the individual will enter any additional information into the Online Immigrant Visa and Alien Registration Application (Department of State Form 260, or DS-260) found on the Consular Electronic Application Center (CEAC) website. (Note: CEAC is not within the boundary of VAMS).

eDP/eDP Web: Information is submitted to the NVC via forms and documents mailed by the IV applicant, petitioner or legal representative. Documents are scanned or uploaded into eDP via an eDP client workstation application. Once collected via eDP, the information can be viewed via eDP Web.

The following forms collected via eDP may contain PII:

DS-0234, Special Immigrant Visa Biodata Form
DS-157, Supplemental Nonimmigrant Visa Application

DSP-122, Supplemental Registration for the Diversity Immigrant Visa Program
I-797, Notice of Action
I-864, Affidavit of Support under Section 213A of the INA
I-864A, Contract between Sponsor and Household Member
I-864EZ, Affidavit of Support under Section 213A of the INA
I-864W Request for Exemption for Intending Immigrant's Affidavit of Support
I-130, Petition for Alien Relative
I-800 Petition to Classify Convention Adoptee as an Immediate Relative
I-526 Immigrant Petition by Alien Entrepreneur
I-129F Petition for Alien Fiance/Spouse
I-600 Petition to Classify Orphan as an Immediate Relative
I-730 Refugee/AsyleeRelative Petition
I-360 Petition for Amerasian, Widow(er), or Special Immigrant
I-929 Petition for Qualifying Family Member of a U-1 Nonimmigrant
I-140 Immigrant Petition for Alien Worker
I-600A Application for Advance Processing of an Orphan Petition
I-824 Application for Action on an Approved Application or Petition

IVIS: The information is provided by an individual who submits an immigration petition to USCIS via paper form. USCIS reviews and adjudicates the petition and forwards the approved petitions (in paper form) to the State Department NVC located in Portsmouth, NH for visa processing and scanned into IVIS.

Some of the petitioner's data is transferred electronically to IVIS via DataShare, which provides high performance secure connectivity between the State Department and DHS to support the exchange of visa data. A third party source of additional information is the commercial bank under State Department contract. A text file from the commercial bank with case numbers is used to track the payments from the petitioners.

Updates to PII information are submitted to the NVC via forms (I-129, I-130, I-360, I-140, I-526, I-600, I-600A, I-730, I-800/800A, I-824, or I-929) and documents mailed by the petitioner or legal representative to the NVC, as well as through telephone and email exchanges.

PIVOT: Petitioner and applicant PII is obtained from an individual petitioner who submits a petition (via one of the following forms: I-129, I-130, I-360, I-140, I-526, I-600, I-600A, I-730, I-800/800A, I-824, or I-929) for immigration of the visa applicant to the USCIS. Petitions are filled in online in USCIS web systems outside of the Department of State. USCIS reviews and adjudicates the petition and forwards the approved petitions

(presently in paper form) to Department of State National Visa Center (NVC). NVC data is also stored in the CCD. Alternatively, PIVOT receives the forms from IVIS electronically when a petition is from a Post that PIVOT is deployed at.

Some of the petitioner's data is transferred electronically to PIVOT via the CCD, which provides high performance secure connectivity between the Department of State and Department of Homeland Security (DHS) to support the exchange of visa petition data. Updates to PII are submitted to the NVC electronically and via paper forms. The petitioner, applicant or legal representative can complete the paper Immigrant Visa Application Form, DS-230, or the electronic DS-260 available in CEAC. Information may also be collected through telephone and email exchange. Public inquiry response agents will then update the applicant's records within PIVOT.

(c) Where is the information housed?

☒Department-owned equipment

☐FEDRAMP-certified cloud

☐Other Federal agency equipment or cloud

☐Other

- If you did not select "Department-owned equipment," please specify.

(d) What process is used to determine if the information is accurate?

DVIS: After initial data collection via eDV-AES and DS-260 in CEAC, a consular representative reviews the record to verify the accuracy of the information entered.

eDP/eDP Web: After documents are scanned into eDP, quality assurance is performed to ensure the documents were scanned in correctly. Once documentation is viewable in eDP Web, an accuracy check is performed. After comparing and verifying the electronic documents against the originals obtained during the post interview, an eDP Web user at post who is designated as an Immigrant Visa Overseas Foreign Service Officer (IVO/FSO) then marks the electronic document as "Original Seen and Compared". This is the only type of user in eDP Web who is able to mark documents. Accuracy is the responsibility of the IV applicant. Any errors or omissions detected during the IV application review process are called to the attention of the applicant.

IVIS: There are two main accuracy checks: (1) IVIS has built-in functionality to validate and check on the data being entered, and (2) Visa Processing Specialists review petitions to ensure all required data is provided. A letter is sent to applicants requesting any

inaccurate or missing data be updated or provided. Examples of the information being checked during the review process include:

- Date of birth is compared with the birth certificate provided by the applicant.
- Financial data on the I-864 form is compared with tax returns from the last three years provided by the applicant.

PIVOT: Accuracy of the information on an immigrant visa application is primarily the responsibility of the applicant or representative filing on behalf of the applicant. Contract staff or Department personnel at NVC visually validate the authenticity and the completeness of the information received on the applicant from CEAC, Forms DS-230, and DS-260 before transferring the case to post. PIVOT's workflow includes quality check processes where critical data elements are confirmed as provided on the petition. Additionally, certain fields are validated for accuracy through comparison of civil or financial documents submitted as part of the application process; e.g,, dates of birth entered are compared to the dates on birth certificates, financial data is compared against tax returns, and date of marriage and marital status are checked against marriage certificates.

(e) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

DVIS: The data in DVIS is current as of the date the applicant submits his/her Form DS-260 application for the program. The initial data comes from eDV-AES. That data is current as of the date of the lottery entry. If the individual is selected, the DS-260 is filled out online at a later date in the CEAC system, which is outside of the boundary for this PIA. If applicants have changes to their data, it is corrected via CEAC.

eDP/eDP Web: eDP and eDP Web are not public facing systems. IV applicants may change their information at any time prior to submission of the application. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview.

IVIS: Visa Processing Specialists can pull up petitioner, applicant, and attorney/agent information on their screen to review and validate the data. They also compare the data on the actual paper form with the data received from DHS/USCIS electronically. Changes to data are the responsibility of the applicant who notifies USCIS by submitting the AR-11, Alien's Change of Address Card, (outside of the Department of State).

PIVOT: The case data initially captured in the PIVOT system is derived from the petition form submitted to USCIS by the U.S. citizen or Legal Permanent Resident (LPR) petitioner. As the case progresses and becomes eligible for processing by the Department of State, the PIVOT application interfaces with the Consular Electronic Application Center (CEAC) public-facing site to collect updated information on both the petitioner and applicant(s). Through CEAC, the individuals enter data and upload documentation that is transferred through an established interface via the Consular Consolidated Database (CCD) to the PIVOT system. All updated information is applied to the PIVOT system. (CEAC is not within this logical boundary).

In addition, the National Visa Center (NVC) provides a call center that the individuals may contact to inquire about the data captured and provide updates or corrections as needed.

(f) Does the system use information from commercial sources? Is the information publicly available?
DVIS, eDP/eDP Web, IVIS and PIVOT do not use commercial or publicly available information.

(g) Is notice provided to the individual prior to the collection of his or her information?

DVIS: Not required in this system. The information is collected by eDV-AES and CEAC using the online DS-260 which transfers to DVIS. CEAC would need to provide the notice (and is not within the boundary of this PIA).

eDP/eDP Web

Although EDP/EDP WEB processes documents with the citizen data that is subject to Privacy Act and non-citizen data that is subject to INA 222(f), the systems are not public-facing. The data is provided from the public via electronic upload to CEAC or from other systems after the citizen or non citizen provides documents to DHS or State via email or during an in-person interview. Notification would be part of the CEAC or DHS systems which are outside the scope of the VAMS.

IVIS: IVIS data is collected by other CA systems or other agencies. The DS-260, Online Immigrant Visa and Alien Registration Application, and DS-261, Online Choice of Address and Agent), are filled out and submitted via CEAC (which is not within the boundary of this PIA). CEAC would need to provide the notice.

PIVOT: PIVOT does not collect information directly from persons. Various USCIS paper forms (I-130, I-140, I-129F, I-360, I-536, I-600, I-600A, I-824, I-800/A, I-929) provide a Privacy Act statement. USCIS would need to provide the notice (which is not within the boundary of this PIA).

(h) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, **how** do individuals grant consent?

eDP/eDP Web: These systems are not accessed directly by the public, but have data entered into them from forms the applicant fills out. Applicants, petitioners or legal representatives are provided a Privacy Act statement on the form including consequences for failing to provide data.

- If no, why are individuals not allowed to provide consent?

DVIS, IVIS, PIVOT are not accessed by applicants and they contain data collected from other systems/agencies that would provide the notice and consent at the collection point.

(i) How did privacy concerns influence the determination of what information would be collected by the system?
The PII items collected by these systems are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the PII data in VAMS is to support the State Department's Diversity Visa Program, allow scans of documents to support and track immigrant visa (IV) applications, allow post personnel and DHS to view the supporting documents, communicate with the applicants, and support pre-processing actions for an IV application.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes – each system collects the information for the State Department's Immigrant Visa and Diversity Visa Programs. The collection is related to visa application submission, processing, and approval/denial decisions.

(c) Does the system analyze the information stored in it?

☒Yes **(IVIS)**

☒No **(DVIS, eDP/eDP Web, PIVOT)**

If yes:

(1) What types of methods are used to analyze the information?
IVIS: Compare and contrast methods are used to analyze the information. The analysis results in numerous reports, case status updates (current, non-current, ready for next action), and initiates communications to case beneficiaries (welcome packets, letters requesting additional information, fee bills).

(2) Does the analysis result in new information?
IVIS: Case-related tables will be updated, case notes may be placed on a case if appropriate, and dates of actions taken will be recorded on the case history.

(3) Will the new information be placed in the individual's record? ☒Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

New information is workflow related and does not determine the individual's eligibility to receive a visa.

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

DVIS interfaces with electronic Diversity Visa (eDV), the Consular Consolidated Database (CCD), the Immigrant Visa Overseas (IVO) applications, and Immigrant Visa

Allocation Management System (IVAMS). All of these are **internal** systems used by Department of State personnel working domestically and overseas in connection with processing diversity immigrant visa applications.

eDP/eDP Web shares data with other **internal** Department of State systems: Consular Consolidated Database (CCD); Immigrant Visa Information System (IVIS); Immigrant Visa Overseas (IVO).

IVIS information is shared **externally** with United States Citizenship and Immigration Services (USCIS) via DataShare/Interagency Data Exchange Application (IDEA). IDEA provides application case data from the petition. This data arrives daily and is manually loaded into IVIS. This data is automatically populated in IVIS when creating a new case.

IVIS allows USCIS to share information collected on immigrant petitions and applicants. EDP Web application is used by USCIS for viewing electronic documents. EDP Web is accessed by USCIS through the CCD.

Internally, IVIS shares with the Bureau of Population, Refugees and Migration's (PRM) Worldwide Refugee Admission Program System (WRAPS). The NVC uses IVIS to share immigrant visa petitions data with the Refugee Processing Center's WRAPS system.

IVIS also shares **internally** with other Bureau of Consular Affairs (CA) systems:

- Consular Consolidated Database (CCD) – Conduit for data exchange between IVIS and DataShare/IDEA.
- Immigrant Visa Allocation Management System (IVAMS) – The case number, Foreign State of Chargeability (FSC), post code, and visa class are loaded into IVAMS for the purpose of immigrant visa tracking and reporting.
- Diversity Visa Information System (DVIS) – Alien numbers generated in IVIS are transferred to DVIS and the DV post systems.
- Immigrant Visa Overseas (IVO) – data on immigrant visas, petitions, and allocations is sent to a post location and loaded into their IVO systems.
- SharePoint - data and images on immigrant visas, petitions, and appointment information is shared with a post through a secure site.

PIVOT shares information **internally** with: Consular Consolidated Database (CCD), Consular Affairs/Consular Systems and Technology (CA/CST) Consular Affairs Enterprise Service Bus (CAESB), Immigrant Visa Allocation and Management System (IVAMS), Immigrant Visa Information System (IVIS), Enterprise Appointment

Management System (EAMS), Consular Electronic Application Center (CEAC), Immigrant Visa Overseas (IVO).

(b) What information will be shared?

DVIS: Personal/biographic information about Diversity Visa applicants, status of applications, and appointment letters for applicants who are selected for further processing.

eDP/eDP Web: Scans of supporting documents and/or bin files are shared and uploaded at NVC which can then be replicated to CCD to allow posts to view this supporting documentation. In addition, eDP Web interfaces with CCD to allow a subset of CCD users to view eDP data. The subset of CCD users is for those who have been given access to the IV/DV (Diversity Visa) Applicant Full and IV/DV Applicant Summary reports on CCD. Views of IVIS data are used to associate the eDP data to the IVIS case/applicant; IVIS is also used by eDP to identify the type of eDP user by his/her role. IVO receives bin file data from eDP by way of CCD when IVO shadow tables are populated by bin files from CCD.

IVIS shared data includes petitioner and/or applicant full name, address, email address, telephone number, date of birth, country and city of birth, gender, marital status, Alien number, Social Security number (SSN), tax ID, organization name, U.S. Status (immigration/citizenship status in the United States), nationality, income information for joint sponsors, and electronic documents (PDF and JPG of documents) that support the application.

PIVOT: The data from PIVOT is replicated to the CCD (PIVOT receives USCIS applicant data). The Petition Data Query (PDQ) Electronic Service Bus (ESB) service monitors the PIVOT request log for new requests for USCIS data. PIVOT executes a procedure to export the demand data that is delivered to IVAMS via email and marks the PIVOT records as reported. Case data from non-current IVIS cases that are about to become current is migrated from IVIS to PIVOT. Limited information about current IVIS cases that are ready to be scheduled for interview appointments is sent to PIVOT and forwarded to Enterprise Appointment Management System (EAMS). The PIVOT system updates the Consular Tracking (CTRAC) tables on the local database that are replicated using Oracle Replication first to the CCD and then on to the CEAC DMZ (Demilitarized Zone) database. Backend processes on the CCD monitor incoming replicated data from PIVOT for cases in Transfer Ready status then execute the procedures to populate IVO shadow tables that are pushed out to the target post via Oracle Replication.

(c) What is the purpose for sharing the information?

DVIS: The purpose for sharing the information is to manage and track the Diversity Immigrant Visa process.

eDP/eDP Web:

- CCD - so that IV supporting documents (including bin files) uploaded at NVC can be replicated to allow posts to view this supporting documentation.

- IVIS- associate the eDP data to the IVIS case/applicant; IVIS is also used by eDP to identify the type of eDP user by his/her role

- IVO- to shadow tables

IVIS: The immigrant visa process starts and ends with USCIS. The Department of State does processing after the petition is filed with USCIS and before the visa is actually issued by USCIS. The data is shared between the agencies to complete the business process of issuing immigrant visas.

PIVOT: The data is shared with posts to facilitate the adjudication of visas by consular officers.

(d) The information to be shared is transmitted or disclosed by what methods?

DVIS, eDP/eDP Web, PIVOT: The information is shared by secured internal connections with other consular systems (CCD, IVO, CEAC, IVAMS, eDV), and email. All of these activities and systems reside on the Department's secure intranet network, OpenNet. Information shared externally is exchanged through the CCD and utilizes connection security and agreements. All physical records containing PII are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only.

IVIS: Information is shared internally by replication to the CCD or via text files emailed to posts (IVO). Reports are generated monthly, emailed to the Visa Office, and input into IVAMS (non citizen/non LPR data). Information shared externally (outside boundary) is done by the State Department's secure intranet, OpenNet which allows the NVC to utilize DataShare for the data from the CCD. DataShare allows text files to be converted into Interagency Data Exchange Application (IDEA) format and transferred to USCIS.

(e) What safeguards are in place for each internal or external sharing arrangement?

DVIS: Internal recipients within the Department of State are required to comply with U.S. government requirements for the protection and use of PII. These safeguarding requirements include, but are not limited to, security training and following internal Department policy for the handling and transmission of "Sensitive but Unclassified" information. In addition, all Department users are required to attend annual privacy and security awareness training to reinforce safe handling practices. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

eDP/eDP Web: Access to electronic files is protected by Personal Identify Verification/Personal Identity Number (PIV/PIN), and is under the supervision of system managers. Regularly administered security/privacy training informs authorized users of proper handling procedures. Physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. An Interface Control Document (lCD) is used to define and disclose transmission formats via OpenNet. The Department of State systems that interface with eDP/eDP Web are strictly controlled by Firewall and Network Intrusion Detection System (NIDS) rule sets that limit ingress and egress to them. All changes are requested from the Firewall Advisory Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

IVIS: Safeguards in place for internal sharing arrangements include secure transmission methods (128-bit data encryption using Secure Socket Layer/Transport Layer Security (SSLv3.1/TLSv1), cryptographic keys, certificates, Hash Authentication, multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers, hand-shaking, header checks), permitted by internal State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. Memorandums of Understanding/Agreement (MOU/MOA) are in place with USCIS. All external communications are encrypted. Regularly administered security and privacy training informs authorized users of proper handling procedures. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

PIVOT: Vulnerabilities are mitigated by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data. The security program involves the establishment of

strict rules of behavior for each major application, including PIVOT. It includes a periodic assessment of physical, technical, and administrative controls designed to enhance accountability and data integrity. It also requires that all users must be adequately trained regarding the security of PIVOT, that system users must participate in a security training program, and that contractors and consultants must also sign a non-disclosure agreement. External connections must be documented and approved with both parties' signature in an Interconnection Service Agreement, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Defense in depth is deployed as well as role based access based on least privilege. Audit trails track and monitor usage and access.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:
Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

2) Strict role based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level

3) System authorization and accreditation process along with continuous monitoring via Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

4) All communications shared with external agencies are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
DVIS, eDP/eDP Web: Applicants do not have access to their information directly on the system; however, procedures for acess and redress are published in the Privacy Act System of Records Notice (SORN) Visa Records State-39, and in rules published at 22 CFR 171 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. In addition, procedures are published on the Department of State public web site, and the Privacy Office website. Applicants are also informed of the process during their visa interview.

IVIS / PIVOT: Users can review the PII text data associated with their visa applications via CEAC, which is external to IVIS and PIVOT, although they cannot view the electronic documents that NVC attached to the case. U.S. citizen and LPR petitioners and sponsors with cases captured by PIVOT may gain access to their information via communication with the National Visa Center (NVC). The NVC provides a call center that individuals may contact to inquire about their case or to make updates and corrections. Applicants may also communicate with the NVC through the Consular Electronic Application Center (CEAC) public-facing site as well as update contact information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
DVIS/eDP/eDP Web: After the case records are sent to overseas posts for further processing, applicants have opportunities to update or correct information through correspondence with post and at the formal interview for the visa. The applicant may initiate updates to his/her information when filling out the DS-260. In addition, as published on travel.state.gov, KCC processes the cases and applicants are able to contact KCC directly. If KCC notices discrepancies in the data, KCC contacts the applicants. The applicants are notified by email to check Electronic Diversity Visa/Entrant Status Check (eDV/ESC). eDV/ESC displays their appointment letter which indicates their post

assignment, the post address, and interview day/time. After that time, they are able to contact post.

IVIS: To correct inaccurate or erroneous information, applicants may contact the National Visa Center (NVC) to update or amend information.

PIVOT: IV applicants may change their information anytime during processing of a case. The IV applicant may submit updates to contact information in the form of email addressed through the CEAC. Until the full IV package and application are submitted, the IV applicant may submit updated information through the CEAC or by contacting the NVC by telephone or email. Processing Specialists at the NVC will update case data at the request of the IV applicant. Processing Specialists at the NVC may also identify discrepancies and send messages through the CEAC requesting updated or corrected information. These corrections are made directly in the CEAC and transferred back to PIVOT through the CCD. Once an application has been submitted, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request, in addition to case status information:

1. Correspondence previously sent to or given to the applicant by post;
2. Civil documents presented by the applicant and
3. Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

If no, explain why not.

(d) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

1. During their visa interview
2. Published SORNs
3. Instructions on forms and web pages (or links to Agency Privacy Policy)
4. Being notified by letter that a correction is needed

Each method contains information on how to amend records and with whom/what office to communicate as well as contact information.

8. Security Controls

(a) How is the information in the system secured?

The system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institures of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a PIV/CAC (Personal Identity Varification/Common Access Card) and PIN (Personal Identification Number) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user

(including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with State Department Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State configuration guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System-Level auditing is set in accordance with the State Department Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system

log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users, including security training and regular refresher training. Each user must annually complete the Cyber Security Awareness Training and pass the Privacy Act PA-459 course, Protecting Personally Identifiable Information. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access or data manupulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?

Awareness that the consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, damage to standing or reputation, financial loss to the Department or individuals, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation.The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

DVIS: State Department personnel (i.e., System/Web Administrators, Application Administrators and Database Administrators) have access to the system and the data. In addition, some members of the development team as appropriate.

eDP/eDP Web: Post consular officers/users, system administrators, and database administrators.

IVIS: The Operations Unit at NVC serves as the administrator for creating and modifying IVIS and eDP accounts, granting the appropriate level of system access based on the determination of the unit manager. In addition, some members of the NVC development team as appropriate, developers and functional leads.

PIVOT: Bureau of Consular Affairs post officers/users, system administrators, and database administrators have access to data in the information system.

(b) How is access to data in the system determined?

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than the administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks and is implemented. Concerning PII, the Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN), and activities while logged in can be traced to the person that performed the activity. Users are aware of this by reading and clicking 'I agree' to the logon banner.